Linear Algebra and its Applications 431 (2009) 1687–1690

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Congruence of symmetric matrices over local rings

Yonglin Cao [a,1], Fernando Szechtman [b,*]

[a] Institute of Applied Mathematics, School of Sciences, Shandong University of Technology, Zibo, Shandong 255091, PR China
[b] Department of Mathematics and Statistics, University of Regina, Saskatchewan, Canada

ARTICLE INFO

Article history:
Received 25 January 2009
Accepted 4 June 2009
Available online 15 July 2009

Submitted by V. Sergeichuk

AMS classification:
15A21
15A33

Keywords:
Matrix congruence
Bilinear form
Local ring
Principal ideal ring

ABSTRACT

Let R be a commutative, local, and principal ideal ring with maximal ideal $\mathfrak{m}$ and residue class field F. Suppose that every element of $1+\mathfrak{m}$ is square. Then the problem of classifying arbitrary symmetric matrices over R by congruence naturally reduces, and is actually equivalent to, the problem of classifying invertible symmetric matrices over F by congruence.

1. Introduction

We consider the problem of classifying symmetric bilinear forms defined on a free R-module of finite rank, where R is a commutative, local and principal ideal ring with maximal ideal $\mathfrak{m}=R\pi$, residue field $F=R/\mathfrak{m}$ and unit group R^*. This is equivalent to the problem of classifying symmetric matrices over R by congruence.

For the ring of integers of a local field of characteristic not 2 the problem was studied by O'Meara [6], who in 1953 gave a complete solution provided 2 is a unit or does not ramify. He also introduced the idea of canonical decomposition of a bilinear form, a concept that will be adopted in this paper.

* Corresponding author.
E-mail addresses: ylcao@sdut.edu.cn (Y. Cao), fernando.szechtman@gmail.com (F. Szechtman).
[1] Research supported by the NNSFC (Nos. 10671151, 6532100).

0024-3795/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2009.06.003

In 1978, Baeza [1] investigated bilinear forms in the more general context of semilocal commutative rings, and we will also have the occasion to use one of his results.

More recently, Levchuk and Starikova [4,5] produced normal forms for quadratic forms over R under certain assumptions on R^*. Their normal forms are of the type introduced by O'Meara, without assuming any sort of completeness.

Our main result, Theorem D, is that, provided $1 + \mathfrak{m} \subseteq R^{*2}$, the problem of classifying arbitrary symmetric matrices over R naturally reduces, and is actually equivalent to, the problem of classifying invertible symmetric matrices over its residue field F.

We require three subsidiary results, namely Lemmas A–C, of which Lemma A is the crucial one. It ensures the uniqueness of O'Meara's canonical decompositions over arbitrary rings R as above. When the form is diagonalizable, and in particular when $2 \in R^*$, this uniqueness is proven in [4] in matrix form. Our proof of Lemma A is independent of [4] and adapted from ideas in modular representation theory, as found in [2,3]. Lemma B -existence of O'Meara's canonical decompositions- is obvious if $2 \in R^*$ and follows from the aforementioned result of Baeza in general. Lemma C establishes a bijection between congruence classes of invertible symmetric matrices over R and F, whenever $1 + \mathfrak{m} \subseteq R^{*2}$. This is probably well-known and is included here for the sake of completeness.

Note that $1 + \mathfrak{m} \subseteq R^{*2}$ as long as $2 \in R^*$ and any one of the following conditions hold: R is Henselian (i.e. Hensel's lemma is true); R is complete; $\mathfrak{m}$ is nilpotent; R is finite. Conversely, if $1 + \mathfrak{m} \subseteq R^{*2}$ then either $\mathfrak{m} = 0$ or $2 \in R^*$. Indeed, suppose $2 \in \mathfrak{m}$ and $1 + \pi$ is a square, say $x^2 = 1 + \pi$. Then $(x-1)^2 \in \mathfrak{m}$, so $x - 1 \in \mathfrak{m}$, whence $x = 1 + a\pi$. Therefore $1 + \pi = x^2 = 1 + 2a\pi + a^2\pi^2$, so $\pi \in \mathfrak{m}^2$, say $\pi = b\pi^2$. Then $\pi(1 - b\pi) = 0$, i.e. $\pi = 0$.

An example of an incomplete local PID satisfying $1 + \mathfrak{m} \subseteq R^{*2}$ is furnished by the ring of integers of the unramified closure of the p-adic numbers, where p is an odd prime.

2. Main results

The ideal $\mathfrak{i} = \cap_{i \geqslant 1} \mathfrak{m}^i$ satisfies $\mathfrak{m}\mathfrak{i} = \mathfrak{i}$, so $\mathfrak{i} = 0$ as above. Hence every non-zero element of R is of the form $\pi^i u$ for some $i \geqslant 0$ and some unit u. Thus, either π is nilpotent, say of degree m, or else R has no zero divisors. We set $M = m$ in the first case and $M = \infty$ in the second. In either case, the non-zero ideals of R are $\mathfrak{m}^i$, where $0 \leqslant i < M$.

Let V and W be free R-modules of positive but not necessarily finite rank. Two bilinear forms $f : V \times V \to R$ and $g : W \times W \to R$ are equivalent, or isometric, if there an isomorphism of R-modules $T : V \to W$ such that $g(Tx, Ty) = f(x, y)$ for all $x, y \in V$. Two matrices $A, B \in M_n(R)$ are congruent if there exists $X \in \mathrm{GL}_n(R)$ such that $X'AX = B$, where X' stands for the transpose of X. In that case we write $A \backsim B$. Clearly f and A respectively give rise to a bilinear form $\overline{f} : V/\mathfrak{m}V \times V/\mathfrak{m}V \to F$ and a matrix $\overline{A} \in M_n(F)$, both defined in an obvious manner. If V has finite rank, say n, then f is non-degenerate if the Gram matrix of f relative to some (and hence every) basis of V belongs to $\mathrm{GL}_n(R)$. In that case $\overline{f}$ is also non-degenerate.

Let $f : V \times V \to R$ be a symmetric bilinear form. Following [6], we say that f has a *canonical decomposition* if there exist a free submodule V_0 of V, possibly zero, as well as a family $(V_i)_{i \in S}$ of non-zero free submodules of V of finite rank, a family of distinct non-negative integers $(a_i)_{i \in S}$ all of which are less than M, and a family of non-degenerate symmetric bilinear forms $f_i : V_i \times V_i \to R$, such that V is equal to the orthogonal direct sum of V_0 and all of the V_i, the restriction of f to V_0 is zero, and the restriction of f to each V_i is $\pi^{a_i} f_i$. This is denoted by

$$f = \perp_{i \in S} \pi^{a_i} f_i \perp f_0. \tag{1}$$

Lemma A. *Let $f : V \times V \to R$ be a symmetric bilinear form defined on a non-zero free R-module. Suppose f admits a canonical decomposition (1). Then the integers a_i, the rank of each V_i, and the isometry type of each $\overline{f_i}$, are all uniquely determined by f, as is the rank of V_0.*

Lemma B. *Let $f : V \times V \to R$ be a symmetric bilinear form defined on a non-zero free R-module of finite rank. Then f admits a canonical decomposition.*

Lemma C. *Suppose* $1+\mathfrak{m}\subseteq R^{*2}$ *and let* $A,B\in \mathrm{GL}_n(R)$ *be symmetric. Then* $A\sim B$ *if and only if* $\overline{A}\backsim\overline{B}$.

Theorem D. *Suppose* $1+\mathfrak{m}\subseteq R^{*2}$. *For each* $k\geqslant 1$, *let* S_k *be a system of congruence representatives of symmetric matrices in* $\mathrm{GL}_k(F)$, *and let* T_k *be any symmetric lift of* S_k *to* $\mathrm{GL}_k(R)$. *Then any symmetric matrix* $A\in M_n(R)$ *is congruent to one and only one matrix of the form* $\oplus_{1\leqslant i\leqslant s}\pi^{a_i}A_i\oplus A_0$, *where* $0\leqslant a_1<\cdots<a_s<M, A_i\in T_{k_i}, A_0$ *is the zero matrix of size* k_0 *– possibly zero –, and* $k_0+k_1+\cdots+k_s=n$.

3. Proofs

Proof of Lemma A. For each $j\geqslant 0$ we consider the submodule $V(j)$ of V, defined by

$$V(j)=\{x\in V\mid f(x,V)\subseteq \mathfrak{m}^j\}.$$

Suppose next that $0\leqslant j<M$. We further define the submodule $N(j)$ of $V(j)$ by

$$N(j)=V(j+1)+((\mathfrak{m}V)\cap V(j))$$

and consider the quotient module

$$W(j)=V(j)/N(j).$$

We finally set

$$V(\infty)=\{x\in V\mid f(x,V)=0\},\quad N(\infty)=(\mathfrak{m}V)\cap V(\infty),\quad W(\infty)=V(\infty)/N(\infty).$$

Note that all $W(j)$ as well as $W(\infty)$ are vector spaces over F.

Let B_0 be a basis of V_0 and let B_i be a basis of V_i for each $i\in S$. Observe that if $0\leqslant j<M$ then $V(j)$ is spanned by all $v\in B_i$ such that $j\leqslant a_i$ together with all $\pi^{j-a_i}v$ such that $v\in B_i$ and $j>a_i$.

As a consequence we obtain first that $W(j)=0$ if j is not equal to any a_i, and second that $W(a_i)$ has an F-basis formed by all $v+N(a_i)$ such that $v\in B_i$. In particular, the rank of V_i is equal to the dimension of $W(a_i)$.

Likewise, we find that $W(\infty)$ has an F-basis formed by all $v+N(\infty)$ such that $v\in B_0$. In particular, the rank of V_0 is equal to the dimension of $W(\infty)$.

Next fix $i\in S$. It remains to see that the isometry type of $\overline{f_i}$ is uniquely determined by f. For this purpose, note first that we have an isomorphism of R-modules, say d_i, from $F=R/\mathfrak{m}$ onto $\mathfrak{m}^{a_i}/\mathfrak{m}^{a_i+1}$, given by $r+\mathfrak{m}\mapsto \pi^{a_i}r+\mathfrak{m}^{a_i+1}$.

Secondly, a careful inspection reveals that the map $g_i: W(a_i)\times W(a_i)\to \mathfrak{m}^{a_i}/\mathfrak{m}^{a_i+1}$,

$$g_i(x+N(a_i),y+N(a_i))=f(x,y)+\mathfrak{m}^{a_i+1},\quad x,y\in V(a_i),$$

is well-defined. It is clearly symmetric and bilinear. Composing g_i with d_i^{-1} produces a well-defined symmetric bilinear form $h_i: W(a_i)\times W(a_i)\to F$.

It is now a routine matter to verify that the F-linear isomorphism $T_i: V_i/\mathfrak{m}V\to W(a_i)$ given by $v+\mathfrak{m}V_i\mapsto v+N(a_i)$ is an isometry, i.e. $\overline{f_i}\backsim h_i$. This completes the proof. □

Proof of Lemma B. We may assume that f is not the zero form. There is one and only one exponent $i\geqslant 0$ such that $f=\pi^i g$ with $\overline{g}\neq 0$. Working over F, we may write $\overline{g}=g_1\perp g_2$, where g_1 is non-degenerate and g_2 is the zero form. By the choice of i the space underlying g_1 is not zero. By [1, Corollary 3.3] we have $g=f_1\perp f_2$, where $\overline{f_1}=g_1$ and $\overline{f_2}=g_2=0$. Hence $f=\pi^i f_1\perp \pi^i f_2$, where f_1 is non-degenerate and the module underlying f_2 is free of rank smaller than the rank of V. The result now follows by induction. □

Proof of Lemma C. Obviously $A\sim B$ implies $\overline{A}\backsim\overline{B}$. Suppose $\overline{A}\backsim\overline{B}$. We wish to show that $A\sim B$. We may assume that $\mathfrak{m}\neq 0$, for otherwise there is nothing to do. As noted earlier, $1+\mathfrak{m}\subseteq R^{*2}$ and $\mathfrak{m}\neq 0$ imply $2\in R^*$. This readily gives $\overline{A}\backsim\overline{D_1}$ and $\overline{B}\backsim\overline{D_2}$, where $D_1,D_2\in \mathrm{GL}_n(R)$ are diagonal. Hence $\overline{D_1}\backsim\overline{D_2}$. It follows that $A\backsim D_1+C_1$, $B\backsim D_2+C_2$ and $D_1\backsim D_2+C_3$, where C_1,C_2,C_3 are symmetric matrices in $M_n(\mathfrak{m})$.

Using $1 + \mathfrak{m} \subseteq R^{*2}$ once more we easily see that if $D \in \mathrm{GL}_n(R)$ is diagonal and $C \in M_n(\mathfrak{m})$ is symmetric then $D \backsim D + C$. We infer that $A \backsim D_1 \backsim D_2 \backsim B$, as required. □

Proof of Theorem D. This follows at once from Lemmas A, B and C. □

References

[1] R. Baeza, Quadratic forms over semilocal rings, Lecture Notes in Mathematics, vol. 655, Springer-Verlag, Berlin, New York, 1978.
[2] R. Gow, The Steinberg lattice of a finite Chevalley group and its modular reduction, J. London Math. Soc. 67 (2) (2003) 593–608.
[3] J. Jantzen, Kontravariante Formen auf induzierten Darstellungen halbeinfacher Lie-Algebren, Math. Ann. 226 (1977) 53–65.
[4] V. Levchuk, O. Starikova, Quadratic forms of projective spaces over rings, Sb. Math., 197 (2006) 887–899.
[5] V. Levchuk, O. Starikova, A normal form and schemes of quadratic forms, J. Math. Sci. 152 (2008) 558–570.
[6] O. O'Meara, Characterization of quadratic forms over local fields, Proc. Natl. Acad. Sci. USA 39 (1953) 969–972.